4-29-00

A

Attorney Docket No. YOR000049US1

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

"Express Mail" Label No.: EL525103058US
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. §1.10 on the date indicated below and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

Date of Deposit: April 26, 2000

Signature: Linda M. Skeleton

APPLICANT(S): Dimitri Kanevsky, Stephane Herman Maes and Alexander Zlatsin

TITLE: METHODS AND APPARATUS FOR TRANSMITTING DATA IN A PACKET NETWORK

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

Enclosed are the following papers relating to the above-named application for patent:

Application - 18 pages of Specification, 7 pages of Claims and 1 page of Abstract
6 Sheets of informal drawing(s)
Declaration and Power of Attorney
1 Assignment with Cover Sheet
Associate Power of Attorney
Information Disclosure Statement with PTO-1449 and cited references
Check in the amount of $1,660.00 to cover the filing fee and recordation fee

CLAIMS AS FILED				
	NO. FILED	NO. EXTRA	RATE	CALCULATIONS
Total Claims	24 -20 =	4	x $18 =	$72
Independent Claims	14 - 3 =	11	x $78 =	$858
Multiple Dependent Claim(s), if applicable			$260 =	$0
Basic Fee				$690
			TOTAL FEE:	$1620

Please file the application and find enclosed a check in the amount of $1,660.00 to cover the filing fee and recordation fee. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 50-0762** as required to correct the error. Duplicate copies of this letter are enclosed.

Please address all correspondence to: **Kevin M. Mason, Ryan & Mason, L.L.P., 90 Forest Avenue, Locust Valley, New York 11560.** Telephone calls should be made to the under-signed attorney at (203) 255-6560.

Respectfully,

Kevin M. Mason

Kevin M. Mason
Reg. No. 36,597
Attorney for Applicant(s)

Date: April 26, 2000
Ryan & Mason, L.L.P.
90 Forest Avenue
Locust Valley, New York 11560

Attorney Docket No. YOR000049US1

COPY

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

PATENT APPLICATION

"Express Mail" Label No.: EL525103058US
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 C.F.R. §1.10 on the date indicated below and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

Date of Deposit: April 26, 2000

Signature: Linda M. Skeleton

APPLICANT(S): Dimitri Kanevsky, Stephane Herman Maes and Alexander Zlatsin

TITLE: METHODS AND APPARATUS FOR TRANSMITTING DATA IN A PACKET NETWORK

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

Enclosed are the following papers relating to the above-named application for patent:

Application - 18 pages of Specification, 7 pages of Claims and 1 page of Abstract
6 Sheets of informal drawing(s)
Declaration and Power of Attorney
1 Assignment with Cover Sheet
Associate Power of Attorney
Information Disclosure Statement with PTO-1449 and cited references
Check in the amount of $1,660.00 to cover the filing fee and recordation fee

CLAIMS AS FILED				
	NO. FILED	NO. EXTRA	RATE	CALCULATIONS
Total Claims	24 -20 =	4	x $18 =	$72
Independent Claims	14 - 3 =	11	x $78 =	$858
Multiple Dependent Claim(s), if applicable			$260 =	$0
Basic Fee				$690
			TOTAL FEE:	$1620

Please file the application and find enclosed a check in the amount of $1,660.00 to cover the filing fee and recordation fee. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 50-0762** as required to correct the error. Duplicate copies of this letter are enclosed.

Please address all correspondence to: **Kevin M. Mason, Ryan & Mason, L.L.P., 90 Forest Avenue, Locust Valley, New York 11560.** Telephone calls should be made to the under-signed attorney at (203) 255-6560.

Respectfully,

Kevin M. Mason

Kevin M. Mason
Reg. No. 36,597
Attorney for Applicant(s)

Date: April 26, 2000
Ryan & Mason, L.L.P.
90 Forest Avenue
Locust Valley, New York 11560

METHODS AND APPARATUS FOR TRANSMITTING DATA IN A PACKET NETWORK

Field of the Invention

The present invention relates generally to packet transmission techniques, and more particularly, to a method and apparatus for transforming packets, such as packets of biometric data, for efficient transmission over a network.

Background of the Invention

A communication network transfers information, such as data, voice, text or video information, among various devices connected to the network, such as telephones and computers,. Information transmitted over a network is often formatted into packets or cells. Packet networks, such as networks using the Internet Protocol (IP), where transmitted data is divided into packets, are widely used. Packets reach their destination by traversing through one or more network elements, such as switches or routers. Packets typically include a header containing, for example, a source address and a destination address, as well as the actual data.

Various forms of data are increasingly distributed over the public Internet and other packet networks. In particular, packet networks are increasingly being utilized by data intensive applications to carry various forms of data, such as voice telephone traffic, using protocols such as the well-known H.323 protocol, and biometric data that is transmitted to confirm or obtain the identity of a person requesting access to a restricted service, device or location. For example, a number of access control mechanisms evaluate biometric information, such as fingerprints, retinal scans or voice characteristics. For a more detailed discussion of such biometric-based access control systems, see, for example, United States Patent Number 5,897,616, entitled "Apparatus and Methods for Speaker Verification/Identification/Classification Employing Non-Acoustic and/or Acoustic Models and Databases," United States Patent Application Serial Number

09/008,122, filed January 16, 1998, entitled "A Portable Information and Transaction Processing System and Method Utilizing Biometric Authorization and Digital Certificate Security," and United States Patent Application Serial Number 09/417,645, filed October 14, 1999, entitled "System and Method for Providing Secure Financial Transactions," each assigned to the assignee of the present invention and incorporated by reference herein.

A number of protocols have been developed to facilitate the transmission of data over a packet network. For a detailed discussion of many such network protocols, see, for example, W. Richard Stevens, UNIX Network Programming (Prentice-Hall, 1990), incorporated by reference herein. The Transmission Control Protocol (TCP) is one protocol used with the well-known Internet Protocol (IP) to send data over the Internet. While the IP protocol handles the actual delivery of the data, the TCP protocol keeps track of the individual packets within a message for efficient routing through the Internet.

For example, when a hypertext markup language (HTML) file is sent from a Web server to a client (user), the TCP program layer in the server divides the file into one or more numbered packets, and then forwards the packets individually to the IP program layer. Although each packet has the same destination IP address, a given packet may get routed differently through the network. At the receiving end (the client program in the user's computer), the TCP program layer reassembles the individual packets and waits until they have arrived before forwarding them as a single file.

The TCP protocol is a connection-oriented protocol. Thus, a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets managed by the IP layer and for reassembling the packets back into the complete message at the receiving end.

The User Datagram Protocol (UDP) is another communications protocol that offers a limited amount of service when messages are exchanged between computers

in a packet network using the Internet Protocol (IP). The UDP protocol is generally faster than the TCP protocol since the UDP protocol does not wait for all the packets to arrive at a destination point before processing the data. Failing to wait for all the packets, however, often causes delayed packets to be effectively lost. Like the TCP protocol, the UDP protocol uses the IP protocol to actually get a data unit (a packet) from one computer to another. Unlike the TCP protocol, however, the UDP protocol does not provide the service of dividing a message into packets and reassembling the packets at the receiving end. Thus, an application program that uses the UDP protocol must ensure that the entire message has arrived and is in the proper sequence. The UDP protocol provides port numbers to help distinguish different user requests and optionally provides a checksum capability to verify that the data arrived intact.

In packet networks, a congestion management policy is required to ensure that sufficient network resources are available in the network to handle the signaling and control of the call. Since individual packets within a message can travel over various routes between a given source and destination, individual packets may be lost or delayed if there is sufficient traffic volume or service interruption along any one such route. Depending on the nature of a given application and the transmission protocols utilized, the loss or delay of one or more packets may be remedied using interpolation techniques to approximate the lost data, or may require the entire message to be retransmitted.

Biometric data that is transmitted to confirm or obtain the identity of a person requesting access to a restricted service, device or location, for example, may be particularly intolerant of such lost or delayed packets. Typically, following the loss or significant delay of packets, the authentication system must request the user to repeat the authentication process, thereby consuming additional time and network resources. When the authentication is performed in connection with a financial transaction, for example, the loss or significant delay of packets may cause transactions to be missed, incomplete or incorrectly completed, especially at times of peak network traffic. Furthermore, such

delays in executing a financial transaction may cause a change in price or product availability by the time the transaction is ultimately completed.

A need therefore exists for an improved method and apparatus for transmitting data in a packet network.

Summary of the Invention

Generally, methods and apparatus are disclosed for transmitting data, such as biometric data or Internet telephone data, in a packet network. The present invention splits and interchanges packets transmitted across a packet network, such that packets that reach their destination may be processed, even in the presence of lost or delayed packets.

In an illustrative biometric embodiment, packets of biometric data, such as fingerprints, retinal scans or voice characteristics, are split, and optionally interchanged prior to transmission. In this manner, if some of the packets are lost or delayed, while some of the packets reach their destination and provided sufficient data for user identification, then the user may be authenticated without requesting the retransmission of the lost or delayed data. Similarly, for the case of packet telephone data, the sampled voice packets are split, and optionally interchanged prior to transmission. In this manner, if some of the packets are lost or delayed, while some of the packets reach their destination, then the received speech samples may be reproduced without requesting the retransmission of the lost or delayed data.

A packet splitter splits framed data into a number of packets. In the illustrative embodiment, the framed data is split into two packets with the first packet containing k frames having odd indexes: f_1, f_3, ... $f_{(2k+1)}$ and the second packet having k frames having even indexes f_2, f_4, ... f_{2k}. If both packets arrive at a destination point, they can be integrated back into the framed data comprised of the continuous string of frames, f_1, f_2, f_3, ..., f_N. Otherwise, if a packet was lost or significantly delayed, the data can be recovered from the single received packet using, for example, smoothing techniques, such as spline extrapolation, for the lost packets with even indexing.

In a further variation, the packet data may be split and interchanged such that compressed biometrics information for two subsequent packets, S1 and S2 is reorganized. Generally, half of packet S1, referred to as S1a, is switched with half of packet S2 , referred to as S2a, before transmitting the data. S1a consists of every other frame of digitized voice signal. The second half of S1, referred to as S1b, consists of all the remaining frames of S1 that are not in S1a. S2 is split into two parts, S2a and S2b, in a similar manner. After switching S1a with S2a, two new packets are produced, where packet P1 contains parts S2a and S1b and packet P2 contains parts S1a and S2b. The new packets P1 and P2 are sent over the network 110 instead of S1, S2. If at a destination point, both packets P1 and P2 arrive the packets P1 and P2 will be reconstructed to form packets S1 and S2 from P1 and P2 by switching S1a and S2a. If only one packet, such as packet P1, arrives, then the content of packet P1 will be split in two packets and loss information will be extrapolated. In this manner, only some reduction in voice quality will happen instead of full loss of information.

A more complete understanding of the present invention, as well as further features and advantages of the present invention, will be obtained by reference to the following detailed description and drawings.

Brief Description of the Drawings

FIG. 1 illustrates a network environment in which the present invention can operate;

FIG. 2 illustrates a packet splitter that may be utilized by a source server of FIG. 1, in accordance with the present invention;

FIGS. 3A through 3D illustrate various representative biometric portions, applicable to one embodiment of the present invention;

FIG. 4 illustrates the splitting of biometric portions, in accordance with one embodiment of the present invention;

FIG. 5 is a schematic block diagram of a biometric integrator that may be utilized by a destination server of FIG. 1, in accordance with the present invention;

FIG. 6 is a schematic block diagram of an integrator that may be utilized by a destination server of FIG. 1, in accordance with the present invention; and

FIG. 7 is a flow chart describing a packet splitting process in accordance with the present invention.

Detailed Description of Preferred Embodiments

FIG. 1 illustrates a network environment 100 in which the present invention can operate. According to one feature of the present invention, packets that are transmitted across the network 110 are split and interchanged, such that packets that reach their destination may be processed, even in the presence of lost or delayed packets. While the present invention may be applied to any information transmitted over a packet network, the invention is illustrated herein using Internet telephone and biometric data as examples.

In the case of biometric data, such as fingerprints, retinal scans or voice characteristics, the biometric data packets are split, and optionally interchanged prior to transmission. In this manner, if some of the packets are lost or delayed, while some of the packets reach their destination and provided sufficient data for user identification, then the user may be authenticated without requesting the retransmission of the lost or delayed data. The present invention recognizes, for example, that a frame-by-frame speaker recognition system can directly be performed on portions of the biometric data.

Similarly, for the case of packet telephone data, the sampled voice packets are split, and optionally interchanged prior to transmission. In this manner, if some of the packets are lost or delayed, while some of the packets reach their destination, then the received speech samples may be reproduced without requesting the retransmission of the lost or delayed data.

In one embodiment shown in FIG. 1, a first packet telephone 130-1 communicates over the packet network 110 with a second packet telephone 130-2. As previously indicated, the voice communications may conform, for example, to the H.323 protocol. As discussed further below in conjunction with FIG. 2, the voice packets are split and optionally interchanged in accordance with the present invention. When a user calls over the network 110, such as the Internet, using a packet telephone 130-1 to a destination packet telephone 130-2, the voice telephone data is received by a server 115-1. The voice data is split into packets 1-3 by a packet splitter (not shown in FIG. 1), discussed further below in conjunction with FIG. 2, each routed by the server 115-1 along separate paths 112-1 through 112-3. Thereafter, the network 110 delivers the packets 1-3 to the server 115-2 associated with the destination device 130-2 using separate paths 118-1 through 118-3. As shown in FIG. 1, if one of the packets, such as packet 2, does not reach the destination device 130-2, the destination device 130-2 can still reproduce the received voice data associated with packets 1 and 3 for the user. The quality of the telephone data received at the destination device 130-2 degrades insignificantly despite the loss of one or more packets.

In one embodiment shown in FIG. 1, a central biometric security system 180 restricts the ability of a user operating a computing device 120 to access a device, such as a server 170, that is connected to the network 110. It is noted that while the illustrative embodiment of the present invention utilizes a remote biometric security system 180 to restrict access to a remote device 170, the present invention can likewise be applied to restrict access to a local device 170, or to a local secure facility or service, as would be apparent to a person of ordinary skill in the art.

The biometric security system 180 uses biometric data about the user, obtained, for example, from a biometric sensor unit 140, to verify the identity of the user. According to a feature of the present invention, discussed further below in conjunction with FIG. 3, the biometric data is split and optionally interchanged in accordance with the present invention. In this manner, only a portion of the biometric data may be used to

validate the user's identity. For a more detailed discussion of biometric portions, see United States Patent Application Serial Number 09/467,581, filed December 20, 1999, entitled "Methods and Apparatus for Restricting Access of a User Using Random Partial Biometrics," assigned to the assignee of the present invention and incorporated by reference herein.

The partial biometrics data is provided to the server 115-1 and split into packets by a splitter (not shown in FIG. 1), discussed further below in conjunction with FIG. 2. Each packet is routed by the server 115-1 along separate paths 112-1 through 112-3. Thereafter, the network 110 delivers the packets 1-3 to the server 115-2 associated with the central biometric system 180 using separate paths 118-1 through 118-3. As shown in FIG. 1, if one of the packets, such as packet 2, does not reach the central biometric system 180, the central biometric system 180 can still process the received biometric data associated with packets 1 and 3 to identify the user. The quality of the biometric data received at the destination device 130-2 degrades insignificantly despite the loss of one or more packets.

The user biometric data is obtained, for example, from a camera 150 or microphone 160. While the biometric sensor unit 140 is shown as a separate device from the computing device 120, the biometric sensor unit 140 could be integrated in a single device with the computing device 120. The user biometric data can include fingerprints, voice characteristics, facial characteristics, handwriting characteristics, tissue characteristics, gestures and any other known biometric data. A biometric prototype database 190 records a biometric prototype for each registered user, in a known manner.

According to one feature of the present invention, a portion of the digitized user biometric data is sent to the central biometric security system 180 using separate packets to validate the identity of the user. The portion of the digitized user biometric data can include a portion of a digitized image, for example, when the biometric data consists of a fingerprint, facial characteristic or handwriting characteristic, or a portion of speech segments when the biometric data consists of voice characteristics.

Network resources are conserved, since only a portion of the original biometric image is transmitted, and encryption is not required.

In one implementation, discussed further below, the central biometric security system 180 transmits a request to the biometric sensor unit 140 containing a sequence of random coordinate pairs corresponding to portions of the digitized image of the biometric information. In an alternate implementation, the central biometric security system 180 can request the biometric portion by specifying a particular feature of the digitized image of the biometric information. For example, the central biometric security system 180 can request specific features or regions to be dynamically determined, such as identified portions of a user's face (i.e., region around the lips or eyes) when the biometric data consists of images or video or identified portions of speech, for example, using word-order, when the biometric data consists of speech.

The biometric sensor unit 140 obtains the full biometric image, and extracts the content of pixels from the full image only at the identified coordinates (or features) for transmission to the central biometric security system 180. For example, for each pixel, the biometric sensor unit 140 can determine whether the pixel has a binary logic value of zero (0) or one (1). The manner in which the biometric portions are configured into packets for transmission is discussed in conjunction with FIG. 3. The central biometric security system 180 compares the received portions of the full biometric image with the corresponding portions of the biometric prototype stored in the biometric prototype database 190 for this user. The user is permitted to access the requested device 170 if the biometric portions match.

A user operating a computing device 120 sends a request to access a remote server 170 over the network 110. The present invention can also be applied to restrict the user's access to the computing device 120 itself. The user request activates the central biometric security system 180 to identify (or verify the identity of) the user.

The central biometric security system 180 compares the received samples of user biometric portions with the corresponding user prototype biometric portions and

allows the user to access the requested remote device 170 if the received user biometric portions match the user prototype biometric portions. It is noted that the central biometric security system 180 can export the comparison task to another server, such as sensor unit 140 or server 190, in the network environment 100.

As shown in FIG. 1, the network environment 100 may also include a network activity monitor 190 to evaluate the amount of traffic on the network 110, preferably in real-time. The monitor 190 summarizes the data on network activity, such as volumes and speed of transactions in the network 110. The network traffic data may also indicate the traffic on each path, such as paths 112 and 118.

SPLITTING PACKET DATA

FIG. 2 is a block diagram of a splitter 200 that is used by a server, such as the server 115-1, to split packets and optionally interchange packets in accordance with the present invention. As shown in FIG. 2, the splitter 200 includes a compressor 210 for compressing received data 205, a framing block 220 for converting the compressed data into a frame representation 230 and a packet splitter 250 for splitting and optionally interchanging packets in accordance with the present invention.

The compressor 210 may compress the data 205, such as pulse-code-modulated (PCM) voice data, into cepstra. See, for example, Jerome R. Bellegarda, "Context-Dependent Vector Clustering for Speech Recognition", Automatic Speech and Speaker Recognition, 133-153 (Kluwer academic Publishers, C-H Lee & F.K. Song eds, 1996.

Compressed data usually is represented as frames, where small amounts of data were captured at some time interval. For example, cepstra is related to some vector of amount of energies at different frequency bands acquired at regular time intervals. Another example of a frame can be related to a representation of data using wavelet techniques. In this approach, data is represented as a sum of wavelets with weighted coefficients. In the example of FIG. 2, frames at different time intervals t_1, t_2, t_3, ... t_N are labeled as f_1, f_2, f_3, ..., f_N.

The packet splitter 250 splits the framed data 230 into packets, such as packets 260, 270. It is assumed that a typical packet 260, 270 consists of k frames. For example, as shown in FIG. 2, the first packet 260 may consist of k frames having odd indexes: f_1, f_3, ... $f_{(2k+1)}$ and the second packet 270 may consist of k frames having even indexes f_2, f_4, ... f_{2k}.

If both packets 260 and 270 arrive at a destination point, they can be integrated back into the framed data 230 comprised of the continuous string of frames, f_1, f_2, f_3, ..., f_N. Otherwise, if a packet, such as packet 270, was lost or significantly delayed, the data can be recovered from the single received packet 260 using, for example, smoothing techniques, such as spline extrapolation, discussed below, for the lost packets with even indexing.

In a further variation, the packet data may be split and interchanged such that compressed biometrics information for two subsequent packets, S1 and S2 is reorganized. Generally, half of packet S1, referred to as S1a, is switched with half of packet S2 , referred to as S2a, before transmitting the data. S1a consists of every other frame of digitized voice signal. The second half of S1, referred to as S1b, consists of all the remaining frames of S1 that are not in S1a. S2 is split into two parts, S2a and S2b, in a similar manner. After switching S1a with S2a, two new packets are produced, where packet P1 contains parts S2a and S1b and packet P2 contains parts S1a and S2b. The new packets P1 and P2 are sent over the network 110 instead of S1, S2. If at a destination point, both packets P1 and P2 arrive the packets P1 and P2 will be reconstructed to form packets S1 and S2 from P1 and P2 by switching S1a and S2a.

If, on the other hand, only one packet, such as packet P1, arrives, then the content of packet P1 will be split in two packets and loss information will be extrapolated. In this manner, only some reduction in voice quality will happen instead of full loss of information.

It is assumed that the audio-signal has a variable gradient. The gradient for a given audio data segment may change slowly or fast. When the gradient is slowly

changing, an original voice data segment can be recovered when it sampled at low rates. In the case of voice data for a speaker recognition system, it can be assumed that speaker data is represented as cepstra. N consecutive packets, where N is greater than 2, are represented as S_1, S_2, ... S_N. Each packet is split into N sub-packets consisting of sub-samples (taken from N sub-samples of an original sample). These sub-packets can then be switched in a similar manner as sub-packets for the case discussed above where each packet was split into two packets (N=2) and new mixed packets would be created. This allows the recovery of the audio signal if a higher percentage of packets is lost. When the gradient is changing fast, packet is copied, rather than split, and several identical copies of a packet are sent. This redundancy compensates for the loss of some packets.

As discussed further below, the packet splitter 250 may employ an algorithm that receives as input the data rate available between the sender and receiver as well as the dominant frequency content and cost functions imposed by the application.

At any time, the amount of buffered data to expedite and the cost of losing this data are estimated to decide between splitting among two or more packets or repeating some packets. Obviously, binary data requires repeating the data, but may wait for a request to retransmit a missing packet from the receiver. Voice can be temporarily down sampled based on the traffic.

Furthermore, the way that the information is split into S1a and S1b can be different than simply by down sampling. Perfect (or quasi-perfect) reconstruction subband coding or wavelet representation may be utilized, thereby directly taking the frequency content into account. Also, it is more directly compressed by classical coding techniques. The advantage of a multi-resolution technique, such as wavelets, is that if you now split up the signal into N components, you can determine the dominant component to send (and possibly repeat) then add details for which it is less important to appropriately transmit them. Not only does it guarantee that the packets are received on the other end, but it also guarantees that the most important packets will arrive in a timely

manner. Thus, even if all details do not arrive immediately, enough information is sent to reconstruct the packet. Indeed, besides packet losses, packet delays are another major concern.

Similarly, voice data associated, for example, with Internet telephone services, can be split and reorganized. The voice telephone data may be represented as cepstra. The cepstra can be split into packets in a similar manner as described above for biometrics data. The quality of the audio data that is recovered from cepstra will degrade insignificantly if one takes out every second frame from cepstra (and replace them with some extrapolations).

If a user requests access to some service, device or facility via server 115-1, the biometrics sensing unit 140, such as a camera, fingerprint scanner or microphone, will capture user biometric data, such as a face image, fingerprint or voice prints. The captured biometrics data is used by the splitter 250 to determine what kind of packet splitting to perform in accordance with the present invention.

At times of low network traffic, for example, the biometrics data may be transmitted using standard Internet protocols, such as the TCP protocol discussed above. At times of moderate network congestion, the packet splitter 250 may reorganize the biometric data before splitting the data into packets, as discussed above in conjunction with FIGS. 2 and 4. At times of heavy network congestion, the packet splitter 250 may distribute a unique biometrics portion, such as packet 1 in FIG. 4, can be distributed among more than 2 packets. Generally, there is an inverse relationship between network traffic conditions and the recommended number of packets used for transmission.

SPLITTING BIOMETRIC PORTIONS

FIG. 3A illustrates representative biometric portions 301-304 of a fingerprint 300. As shown in FIG. 3A, each part 301-304 of a fingerprint 300 is a small rectangular portion of the larger image 300. As shown in FIG. 3B, biometric portions can include sound sub-units that are represented as areas OE 306, and PH 307 of a spectogram 305, for a sequence of phones OE, L, IE, PH. In addition, biometric portions

can include sound sub-units of a given speech phone, such as phone PH 307. For example, a sub-unit of a phone can include portions of a given phone or the whole cepstral feature vector within a phone. As shown in FIG. 3C, biometric portions can include parts 309-310 of a face picture 308. In addition, as shown in FIG. 3D, biometric portions can include parts 312, 313 of a written phrase 311. In alternate embodiments, biometric portions can also include parts of a picture of an eye, parts of spoken phrases, represented as PCM data, parts of cepstra and parts of gestures. As previously indicated, the biometric portion can be explicitly specified by the central biometric security system 180, for example, by specifying certain pixels to include in the biometric portion, or can be dynamically determined, for example, by specifying certain features, such as lips or eyes, to include in the biometric portion.

FIG. 4 illustrates how biometrics data, such as a fingerprint 400, can be split into packets in such a way that each packet contains partial biometrics. As shown in FIG. 4, biometric portions 401-404 of a fingerprint 400 can be applied to the packet splitter 250, discussed above in conjunction with FIG. 2. The packet splitter 250 generates two packets 1, 2. The first packet contains biometric portions 401, 403 and the second packet contains biometric portions 402, 404. The number of packets generated by the packet splitter 250 can vary depending on the required quality and on network conditions. At times of peak network traffic, for example, then the number of packets into which the partial biometrics are split can be increased.

For a discussion of techniques for obtaining user biometrics, see, for example, United States Patent Number 5,895,447, entitled "Speech Recognition Using Thresholded Speaker Class Model Selection or Model Adaptation," United States Patent Application Serial Number 08/788,471, filed January 28, 1997, entitled "Text Independent Speaker Recognition for Transparent Command Ambiguity Resolution and Continuous Access Control," United States Patent Application Serial Number 08/851,982, filed May 6, 1997, entitled "Speaker Recognition Over Large Population With Fast and Detailed Matches," United States Patent Application Serial Number

08/787,029, filed January 28, 1997, entitled "Speaker Model Prefetching," each assigned to the assignee of the present invention and incorporated by reference herein.

The request for a special sample can include coordinates of portions of a biometric that are represented as a domain in a multi-dimensional vector space. For example, a request for a fingerprint sampling from the fingerprint 300 of FIG. 3A, is represented as four coordinates of centers of squares 301-304. The size of each square 301- 304 can also be included in the request. Another example of a request are coordinates of one or more pixels in a biometric that is represented as a domain in a multi-dimensional vector space. For example, as previously indicated, coordinates can be dynamically chosen as pixels in some facial area, for example, that covers an eye or hairs. The content of such a pixel is a color of the coordinate point that represents eye or hair color.

In addition, the biometric security system 180 can request a set of phones from a spoken phrase. For example, if a user password is a spoken phrase, the speech content corresponding to phones can be used to verify the identity of the user. The speech content can be represented, for example, as PCM or cepstral segments corresponding to time intervals for these phones. These time intervals can be identified using speech alignment techniques, such as those described in F. Jelenek, "Statistical Methods for Speech Recognition," (MIT Press, MA, 1998) or using a ballistic labeler, such as the one described in United States Patent Application Serial No. 09/015,150, filed January 29,1998, entitled "Apparatus and Method for Generating Phonetic Transcriptions From Enrollment Utterances," each incorporated by reference herein.

In a further variation, the biometric security system 180 can request speech data segments using a set of sub-phones, phones or classes of phones. Image biometric portions can be requested, for example, as coordinates of fingerprint sub-areas, coordinates of pixels of fingerprints, coordinates of facial sub-areas, coordinates of pixels of a facial area, coordinates of eye sub-areas, coordinates of pixels of an eye area. Similarly, requests for gesture samples can be obtained by sending time moments

indicating when the gesture samples should be taken. For a discussion of a system for performing a multimedia (audio- video) user recognition, see, for example, United States Patent Application Serial No. 09/369,706, filed August 6, 1999, entitled "Methods and Apparatus for Audio-Visual Speaker Recognition and Utterance Verification," assigned to the assignee of the present invention and incorporated by reference herein.

INTEGRATION OF RECEIVED PACKETS AT DESTINATION

FIG. 5 illustrates a biometric integrator 500 that may be used by the destination server 115-2 (or the central biometric security system 180) to reintegrate the received biometric packets. As shown in FIG. 5, the integrator 500 includes a time constraint module 510 that specifies how long to wait until all the packets arrive. For example, if the secure service, device or facility has some limits on user waiting time, then the biometrics packets that have arrived may be processed. The received packets are integrated by the integrator 500 and the central biometric security system 180 processes whatever biometrics data is received. The processing of partial biometrics data was fully described in United States Patent Application Serial Number 09/467,581, filed December 20, 1999, entitled "Methods and Apparatus for Restricting Access of a User Using Random Partial Biometrics," incorporated by reference above.

As shown in FIG. 5, the biometric integrator 500 also includes a reliability estimator 520 that verifies the reliability of the user verification/authentication using partial biometrics data. Generally, if there is a good match of received partial biometrics data with stored biometrics prototypes than the user is granted access. If the mismatch between the received biometrics portions and the stored biometrics prototypes exceeds some predefined threshold then the user is denied access to the requested service, device or facility. Otherwise, the system waits for any remaining packets to arrive or requests more biometrics screening data from the biometric sensor unit 140. The biometric integrator 500 may also include a smoothing module (not shown) that extrapolates the lost frames of biometric data. There are many methods for smoothing lost data. One of suitable method is based on spline extrapolation. For a discussion of spline extrapolation

techniques, see, for example, www.swcp.com/~larrys/spline_patching_tutorial.htm, incorporated by reference herein.

FIG. 6 illustrates an integrator 600 that may be used by the destination server 115-2 (or the destination packet telephone 130-2) to reintegrate the received voice packets. As shown in FIG. 6, the integrator 600 includes a time constraint module 610 that specifies how long to wait until all the packets arrive. The received packets are integrated by the integrator 600 and the packet telephone 130-2 processes whatever voice data is received.

As shown in FIG. 6, the integrator 600 also includes a smoothing module 620 that extrapolates the lost frames of voice data. There are many methods for smoothing lost data. One of suitable method is based on spline extrapolation. For a discussion of spline extrapolation techniques, see, for example, www.swcp.com/~larrys/spline_patching_tutorial.htm, incorporated by reference herein. The integrated and smoothed voice data is uncompressed to an audio signal that is sent to the packet telephone 130-2.

PROCESSES

FIG. 7 is a flow chart describing an implementation of the present invention from a process point of view. As shown in FIG. 7, the data is initially captured during step 705. The data is then converted into a frame representation during step 710. The frames are then organized into packets during step 720, depending on the content of the data and the current network load (as determined during step 715).

The packet data is then transmitted over the network 110 during step 725. The received packets are collected at the destination during step 730. The time constraint module 510, 610 determines when the predefined time threshold is exceeded during step 735. Once the predefined time threshold is exceeded, the received packets are integrated into the whole data during step 740.

Thereafter, a smoothing algorithm, if available, is applied to the integrated data, if necessary, during step 745. The quality of the smoothed data is evaluated during

step 750. If it is determined during step 750 that the smoothed data has insufficient quality for further processing, then retransmission of the data is requested during step 760.

If, however, it is determined during step 750 that the smoothed data has sufficient quality for further processing, then the smoothed data is processed during step 770, without requesting retransmission.

It is to be understood that the embodiments and variations shown and described herein are merely illustrative of the principles of this invention and that various modifications may be implemented by those skilled in the art without departing from the scope and spirit of the invention.

Claims

What is claimed is:

1. A method for transmitting biometric data in a network, comprising the steps of:

obtaining biometric information for a user;

obtaining a plurality of biometric portions from said biometric information; and

transmitting said biometric portions to a destination using a plurality of packets.

2. The method of claim 1, wherein said user is provided access to a requested device, service or facility if said received biometric portions match corresponding biometric prototype portions.

3. The method of claim 1, wherein said biometric information is a biometric image.

4. The method of claim 1, wherein said biometric information includes speech segments.

5. A method for receiving biometric data in a network, comprising the steps of:

receiving a plurality of packets containing biometric portions corresponding to a user;

determining if said received packets provide sufficient data for processing; and

evaluating said received packets if said received packets provide sufficient data for processing.

6. The method of claim 5, wherein said received packets contain data that has been interchanged from a plurality of original packets and wherein said method further comprising the step of integrating said received packets to generate said original packets.

7. A method for transmitting data in a packet network, comprising the steps of:

obtaining at least two packets of data for transmission;

interchanging said data from said at least two packets to obtain at least two interchanged packets; and

transmitting said interchanged packets to a destination.

8. The method of claim 7, wherein said interchanging step further comprises the steps of placing odd numbered frames from said at least two packets into a first interchanged packet and even numbered frames from said at least two packets into a second interchanged packet.

9. The method of claim 7, wherein said interchanging step generates N interchanged packets and wherein said method further comprises the steps of placing every Nth frame in a given interchanged packet.

10. The method of claim 7, wherein said packets of data include telephone data.

11. A method for receiving data in a packet network, comprising the steps of:

receiving a plurality of packets containing data that has been interchanged from a plurality of original packets;

integrating said received packets to generate said original packets;

determining if said received packets provide sufficient data for processing; and

processing said received packets if said received packets provide sufficient data for processing.

12. A method for transmitting data in a packet network, comprising the steps of:

obtaining frames of data for transmission;

generating N interchanged packets by placing every Nth frame of data in a given interchanged packet; and

transmitting said interchanged packets to a destination.

13. The method of claim 12, wherein said frames of data includes biometric.

14. The method of claim 12, wherein said frames of data includes voice data.

15. A system for transmitting biometric data in a network, comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

obtain biometric information for a user;

obtain a plurality of biometric portions from said biometric information; and

transmit said biometric portions to a destination using a plurality of packets.

16. A system for receiving biometric data in a network, comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

receive a plurality of packets containing biometric portions corresponding to a user;

determine if said received packets provide sufficient data for processing; and

evaluate said received packets if said received packets provide sufficient data for processing.

17. A system for transmitting data in a packet network, comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

obtain at least two packets of data for transmission;

interchange said data from said at least two packets to obtain at least two interchanged packets; and

transmit said interchanged packets to a destination.

18. A system for receiving data in a packet network, comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

receive a plurality of packets containing data that has been interchanged from a plurality of original packets;

integrate said received packets to generate said original packets;

determine if said received packets provide sufficient data for processing; and

process said received packets if said received packets provide sufficient data for processing.

19. A system for transmitting data in a packet network, comprising:

a memory that stores computer-readable code; and

a processor operatively coupled to said memory, said processor configured to implement said computer-readable code, said computer-readable code configured to:

obtain frames of data for transmission;

generate N interchanged packets by placing every Nth frame of data in a given interchanged packet; and

transmit said interchanged packets to a destination.

20. An article of manufacture for transmitting biometric data in a network, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to obtain biometric information for a user;

a step to obtain a plurality of biometric portions from said biometric information; and

a step to transmit said biometric portions to a destination using a plurality of packets.

21. An article of manufacture for receiving biometric data in a network, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to receive a plurality of packets containing biometric portions corresponding to a user;

a step to determine if said received packets provide sufficient data for processing; and

a step to evaluate said received packets if said received packets provide sufficient data for processing.

22. An article of manufacture for transmitting data in a packet network, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to obtain at least two packets of data for transmission;

a step to interchange said data from said at least two packets to obtain at least two interchanged packets; and

a step to transmit said interchanged packets to a destination.

23. An article of manufacture for receiving data in a packet network, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to receive a plurality of packets containing data that has been interchanged from a plurality of original packets;

a step to integrate said received packets to generate said original packets;

a step to determine if said received packets provide sufficient data for processing; and

a step to process said received packets if said received packets provide sufficient data for processing.

24. An article of manufacture for transmitting data in a packet network, comprising:

a computer readable medium having computer readable code means embodied thereon, said computer readable program code means comprising:

a step to obtain frames of data for transmission;

a step to generate N interchanged packets by placing every Nth frame of data in a given interchanged packet; and

a step to transmit said interchanged packets to a destination.

METHODS AND APPARATUS FOR TRANSMITTING DATA IN A PACKET NETWORK

Abstract of the Disclosure

Methods and apparatus are disclosed for transmitting data, such as biometric data or Internet telephone data, in a packet network. Packets are split and interchanged prior to transmission across a packet network, such that packets that reach their destination may be processed, even in the presence of lost or delayed packets. Packets of biometric data, such as fingerprints, retinal scans or voice characteristics, are split, and optionally interchanged prior to transmission. If some packets are lost or delayed, while some of the packets reach their destination and provide sufficient data for user identification, then the user may be authenticated without requesting the retransmission of the lost or delayed data. Sampled voice packets are split, and optionally interchanged prior to transmission. If some packets are lost or delayed, while some packets reach their destination, then the received speech samples may be reproduced without requesting the retransmission of the lost or delayed data. A packet splitter splits framed data into a number of packets. For example, the framed data is split into two packets with the first packet containing k frames having odd indexes and the second packet having k frames having even indexes. If both packets arrive at a destination point, they can be integrated back into the framed data comprised of the continuous string of frames, f_1, f_2, f_3, ..., f_N. Otherwise, if a packet was lost or significantly delayed, the data can be recovered from the single received packet using, for example, smoothing techniques, such as spline extrapolation, for the lost packets with even indexing.

1500-100.APP

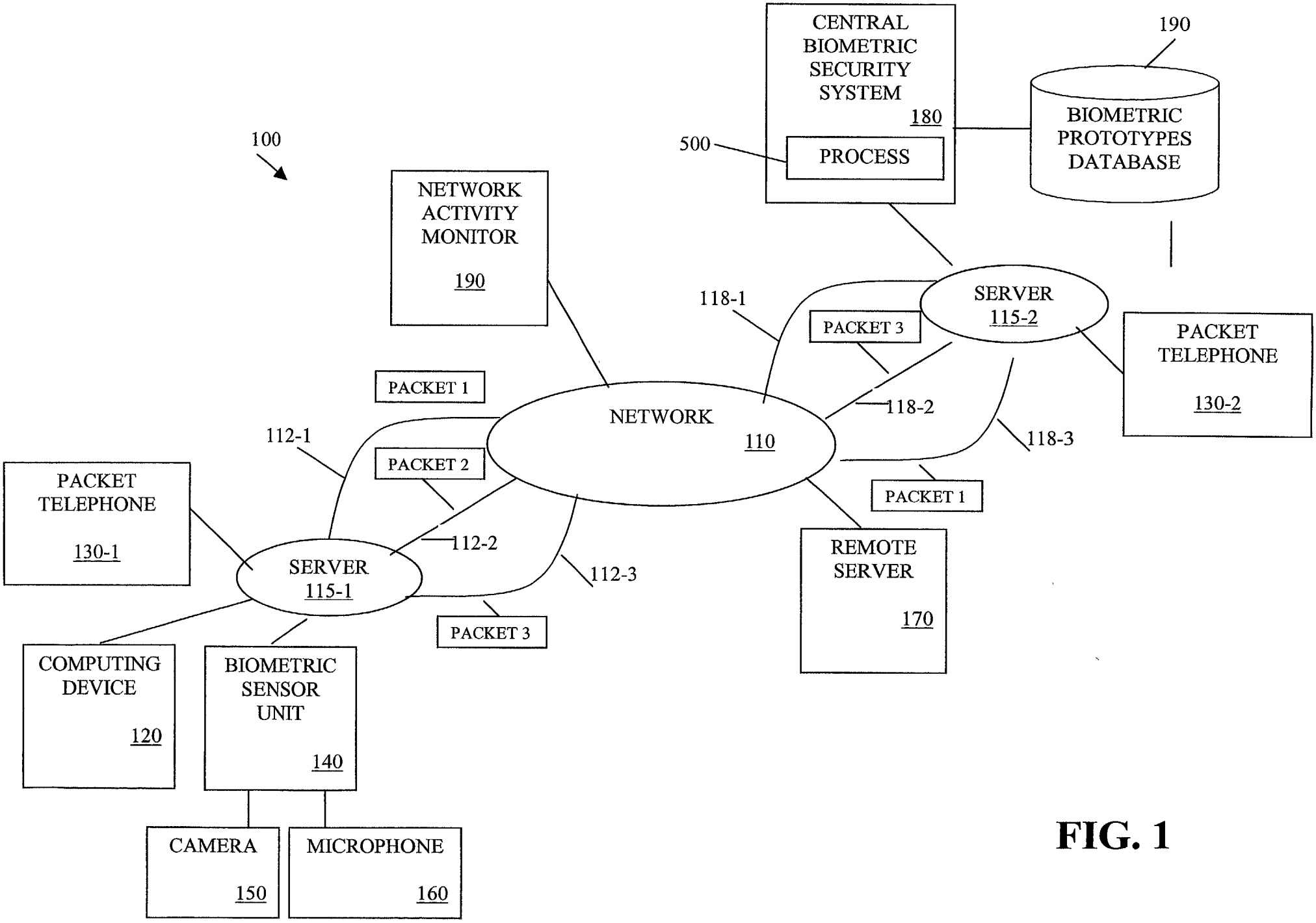

FIG. 1

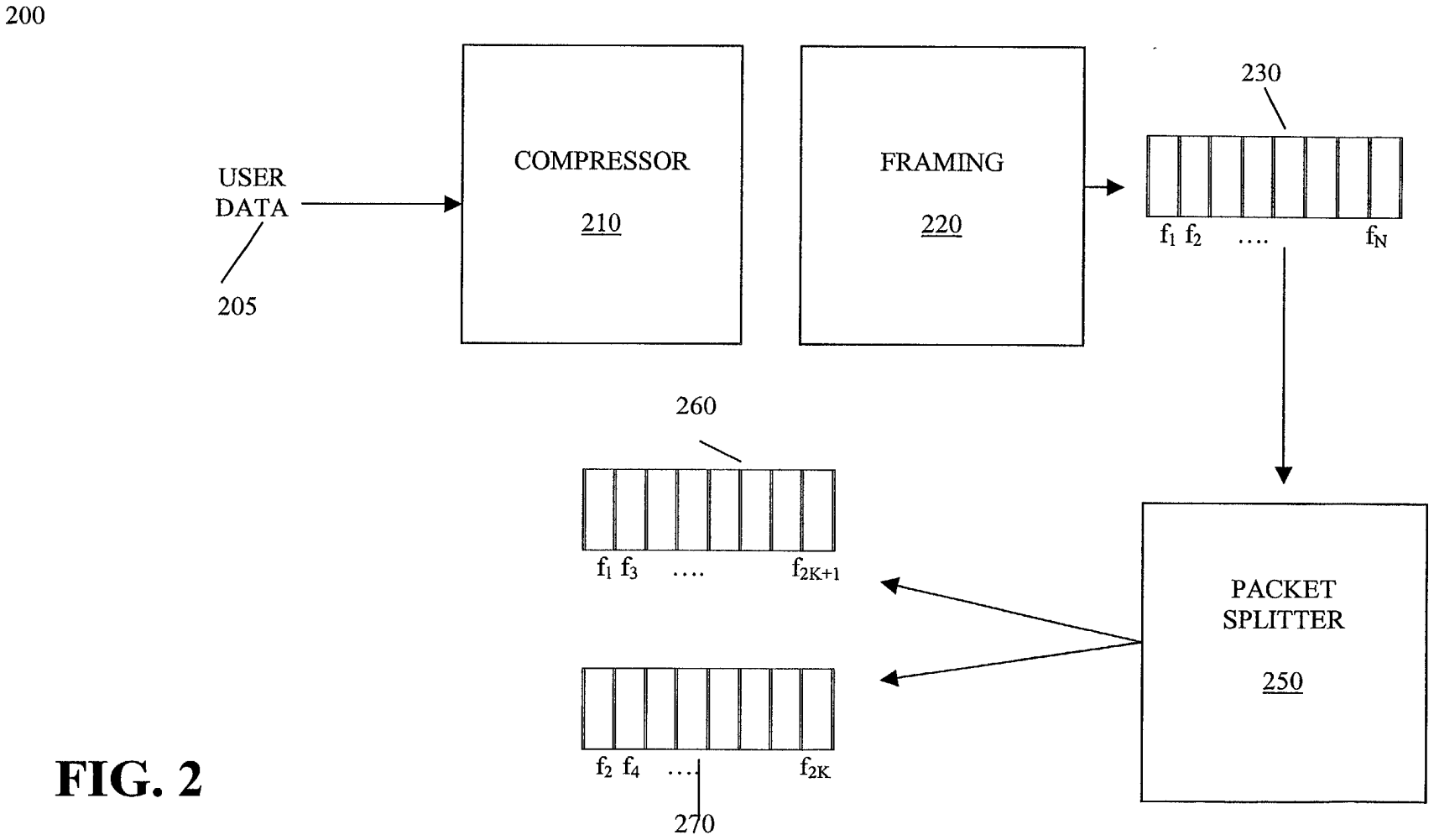

FIG. 2

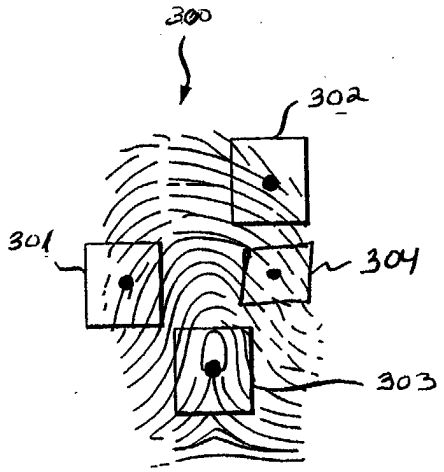

FIG. 3A

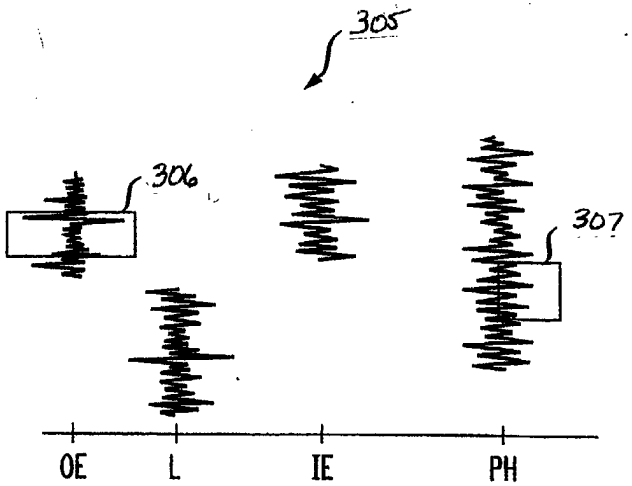

FIG. 3B

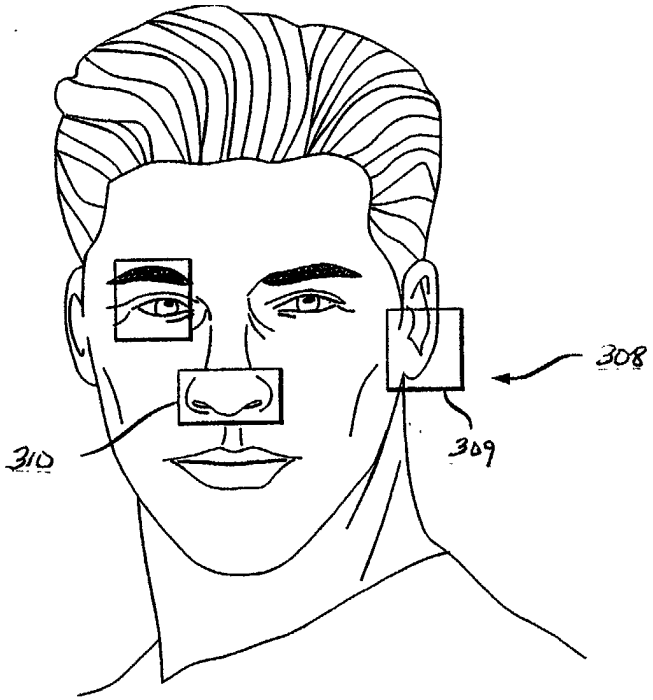

FIG. 3C

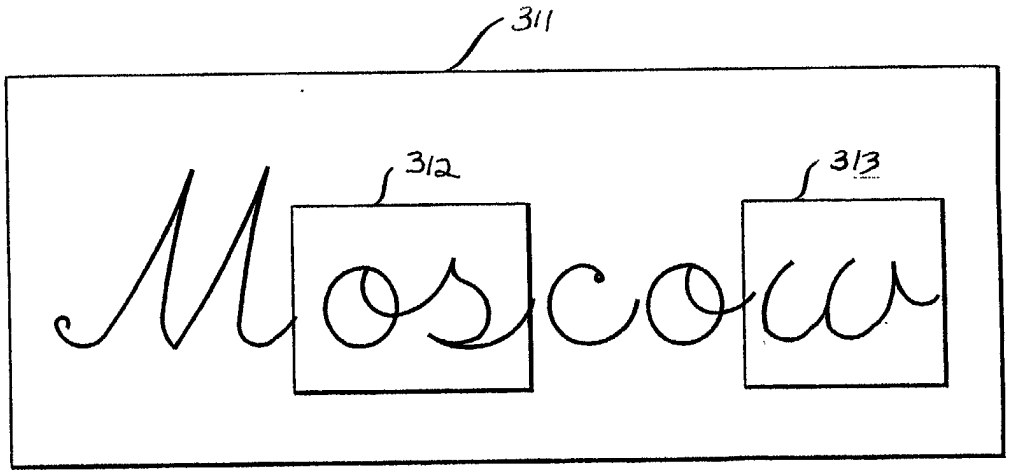

FIG. 3D

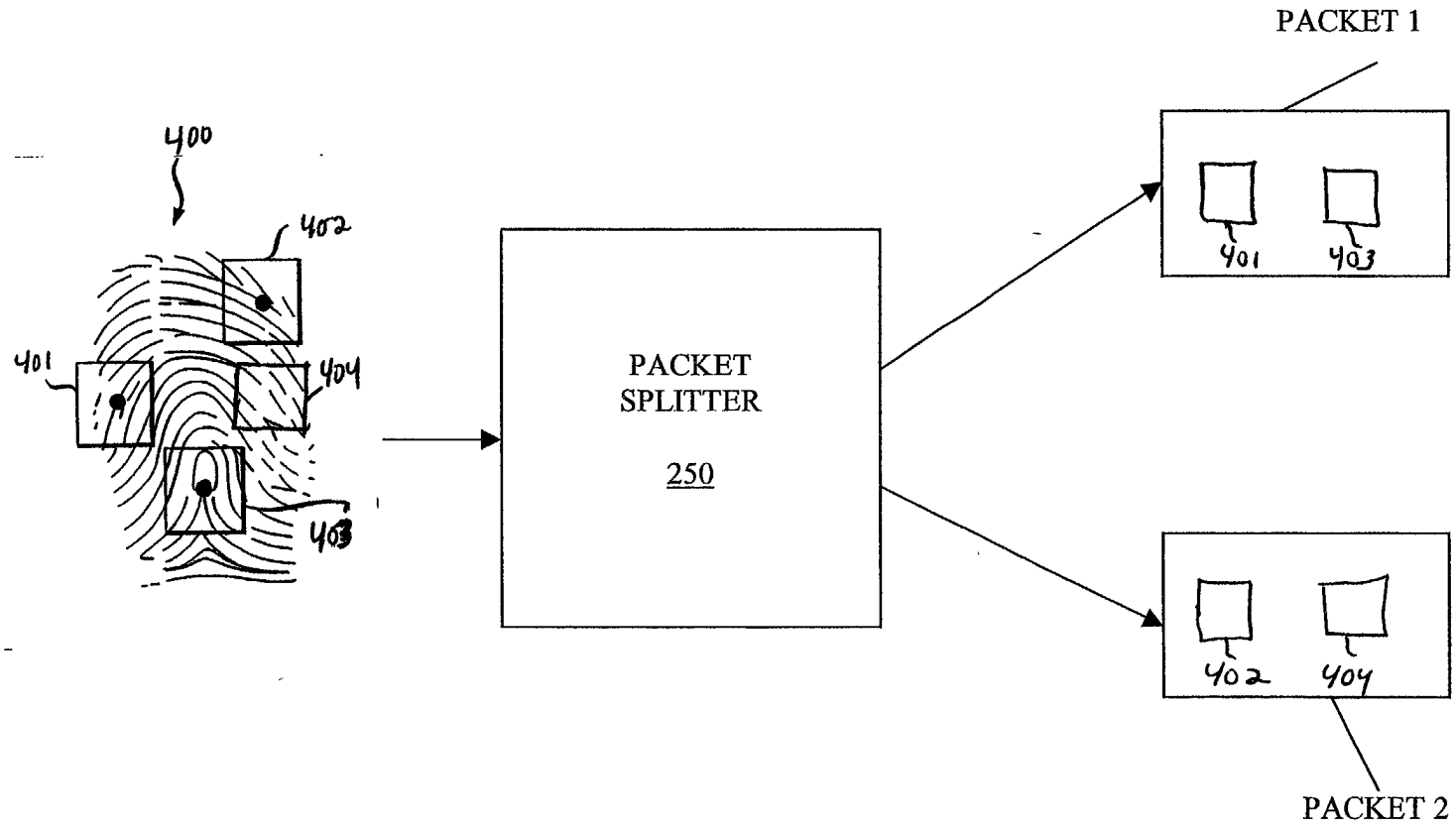
400
402
401
404
403
PACKET
SPLITTER
250
PACKET 1
401
403
402
404
PACKET 2

FIG. 4

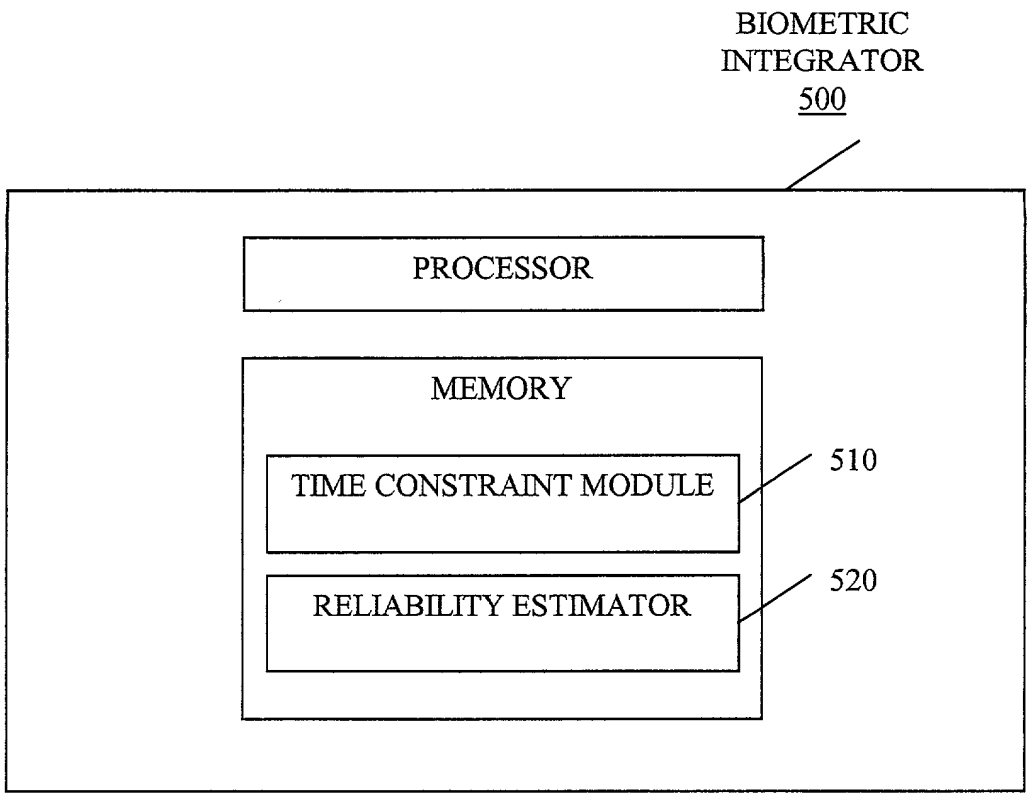
BIOMETRIC
INTEGRATOR
500
PROCESSOR
MEMORY
TIME CONSTRAINT MODULE
510
RELIABILITY ESTIMATOR
520

FIG. 5

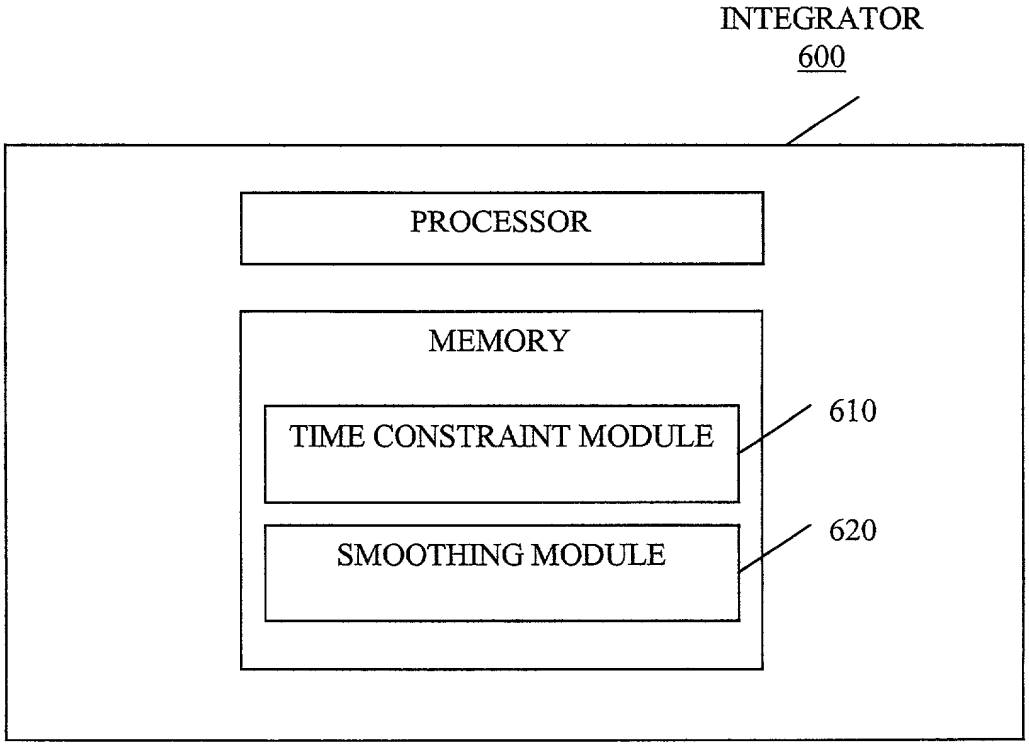
INTEGRATOR
600
PROCESSOR
MEMORY
TIME CONSTRAINT MODULE
610
SMOOTHING MODULE
620

FIG. 6

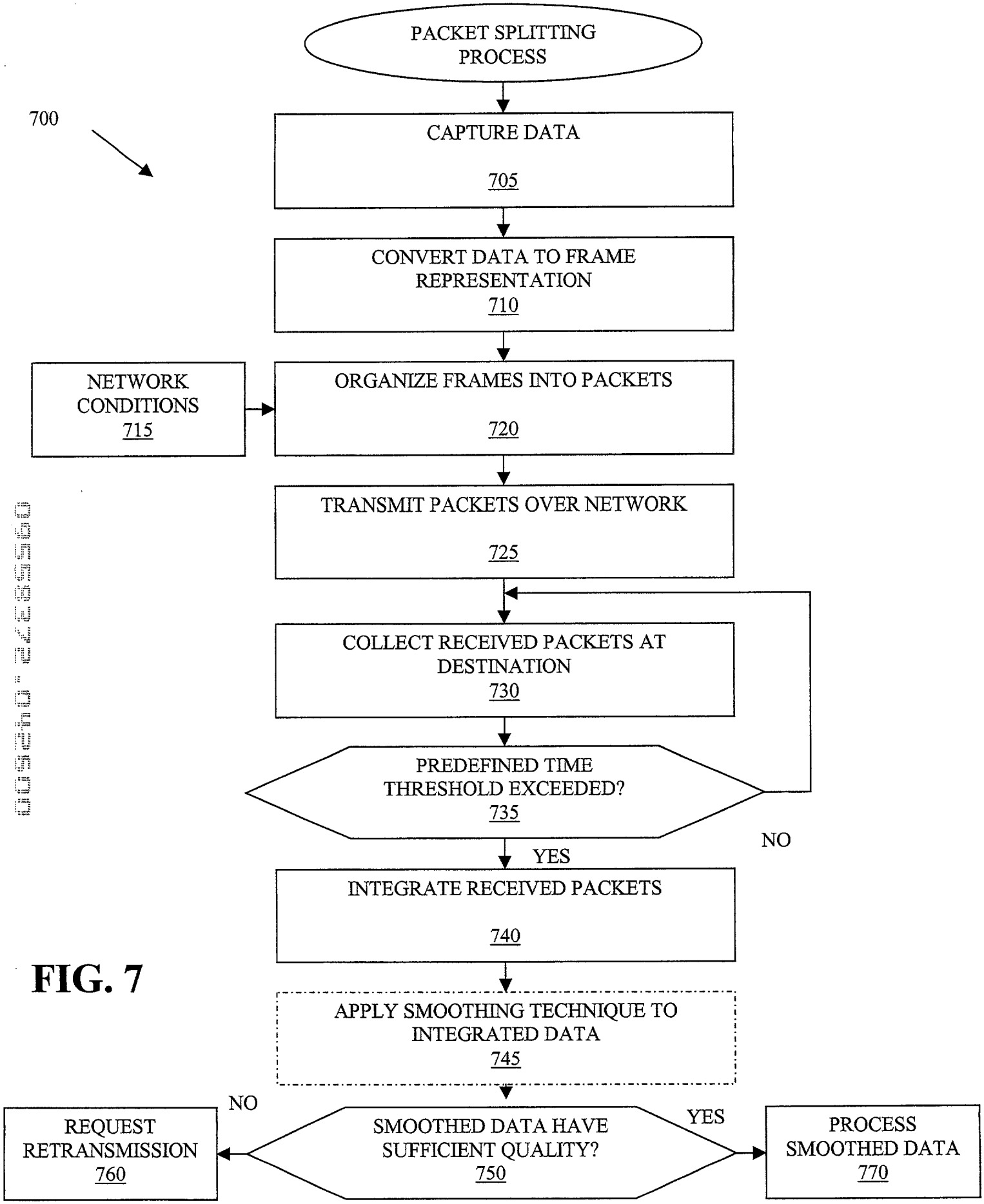
PACKET SPLITTING PROCESS
700
CAPTURE DATA
705
CONVERT DATA TO FRAME REPRESENTATION
710
NETWORK CONDITIONS
715
ORGANIZE FRAMES INTO PACKETS
720
TRANSMIT PACKETS OVER NETWORK
725
COLLECT RECEIVED PACKETS AT DESTINATION
730
PREDEFINED TIME THRESHOLD EXCEEDED?
735
NO
YES
INTEGRATE RECEIVED PACKETS
740
APPLY SMOOTHING TECHNIQUE TO INTEGRATED DATA
745
NO
REQUEST RETRANSMISSION
760
SMOOTHED DATA HAVE SUFFICIENT QUALITY?
750
YES
PROCESS SMOOTHED DATA
770

FIG. 7

DECLARATION

AS A BELOW NAMED INVENTOR, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe that I am the original, first and sole (*if only one name is listed below*), or an original, first and joint inventor (*if plural names are listed below*), of the subject matter which is claimed and for which a patent is sought on the invention entitled:

TITLE: **METHODS AND APPARATUS FOR TRANSMITTING DATA IN A PACKET NETWORK**

the specification of which is attached hereto or indicates an attorney docket no. YOR000049US1, or:

☐ was filed in the U.S. Patent & Trademark Office on _____ and assigned Serial No. _____,

☐ and *(if applicable)* was amended on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability and to the examination of this application in accordance with Title 37, Code of Federal Regulations §1.56. I hereby claim foreign priority benefits under Title 35, U.S. Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States, or §119(e) of any United States provisional application(s), listed below and have also identified below any foreign applications for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

			Priority Claimed:
_____			Yes [ ] No[X]
(Application Number)	*(Country)*	*(Day/Month/Year filed)*	
_____			Yes [ ] No[ ]
(Application Number)	*(Country)*	*(Day/Month/Year filed)*	

I hereby claim the benefit under Title 35, U.S. Code §120, of any United States application(s), or §365(c), of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International applications(s) in the manner provided by the first paragraph of Title 35, U.S. Code §112, I acknowledge the duty to disclose information material to patentability as defined in Title 37, Code of Federal Regulations §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

_____		
(Application Serial Number)	*(Filing Date)*	*(STATUS: patented, pending, abandoned)*
_____		
(Application Serial Number)	*(Filing Date)*	*(STATUS: patented, pending, abandoned)*

I hereby appoint the following attorneys: **MANNY W. SCHECTER**, Reg No. 31,722; **TERRY J. ILARDI**, Reg. No. 29,936; **CHRISTOPHER A. HUGHES**, Reg. No. 26,914; **EDWARD A. PENNINGTON**, Reg No. 32,588; **JOHN E. HOEL**, Reg No. 26,279; **JOSEPH C. REDMOND, Jr.**, Reg No. 18,753; **KEVIN M. JORDAN**, Reg No. 40,277; **STEPHEN C. KAUFMAN**, Reg No. 29,551; **JAY P. SBROLLINI**, Reg. No. 36,266; **DAVID M. SHOFI**, Reg. No. 39,835; **ROBERT M. TREPP**, Reg. No. 25,933; **LOUIS P. HERZBERG**, Reg. No. 41,500; **DANIEL P. MORRIS**, Reg. No. 32,053; **LOUIS J. PERCELLO**, Reg. No. 33,206; **PAUL J. OTTERSTEDT**, Reg. No. 37,411; and **DOUGLAS W. CAMERON**, Reg. No. 31,596; each of them of **INTERNATIONAL BUSINESS MACHINES CORPORATION**, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598; to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith and with any divisional, continuation, continuation-in-part, reissue or re-examination application, with full power of appointment and with full power to substitute an associate attorney or agent, and to receive all patents which may issue thereon, and request that all correspondence be addressed to:

Kevin M. Mason
RYAN & MASON, L.L.P.
90 Forest Avenue
Locust Valley, NY 11560
Tel.: (203) 255-6560

I HEREBY DECLARE that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 U.S. Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF FIRST OR SOLE INVENTOR: Dimitri Kanevsky Citizenship United States of America

Inventor's signature: _____ Date: 4/24/2000

Residence & Post Office address: 1358 Spring Valley Road
Ossining, NY 10562

FULL NAME OF SECOND JOINT INVENTOR: Stephane Herman Maes Citizenship Belgium

Inventor's signature: _____ Date: 4-24-00

Residence & Post Office address: 1 Wintergreen Hill Road
Danbury, CT 06811

FULL NAME OF THIRD JOINT INVENTOR: Alexander Zlatsin Citizenship United States of America

Inventor's signature: _____ Date: 4/24/2000

Residence & Post Office address: 848 Kessler Place
Yorktown Heights, NY 10598

Attorney Docket No. YOR000049US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S): Dimitri Kanevsky, Stephane Herman Maes and Alexander Zlatsin

SERIAL NO.: Unassigned

FILED: Concurrently Herewith

FOR: METHODS AND APPARATUS FOR TRANSMITTING DATA IN A PACKET NETWORK

ASSOCIATE POWER OF ATTORNEY

Please recognize **JOSEPH B. RYAN**, Reg. No. 37,922; **KEVIN M. MASON**, Reg. No. 36,597; and **WILLIAM E. LEWIS**, Reg. No. 39,274; each of them of **RYAN & MASON, L.L.P.**, 90 Forest Avenue, Locust Valley, New York 11560 as associate attorneys in the above-mentioned application, with full power to prosecute said application, to make alterations and amendments therein, and to transact all business in the Patent and Trademark Office connected therewith.

Telephone calls should be made to Kevin M. Mason by dialing (203) 255-6560.

All written communications are to be sent to Kevin M. Mason, Esq., Ryan & Mason, L.L.P., 90 Forest Avenue, Locust Valley, New York 11560.

Dated: APRIL 26, 2000

Paul J. Otterstedt
Registration No. 37,411
Attorney for Applicant(s)

International Business Machines Corporation
T.J. Watson Research Center
Route 134 and Kitchawan Road
Yorktown Heights, New York 10598